UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/739,354	12/18/2003	Chad M. Fors	CE10577R	9648

22917 7590 07/20/2007

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

EXAMINER	
YOUNG, NICOLE M	
ART UNIT	**PAPER NUMBER**
2139	

NOTIFICATION DATE	DELIVERY MODE
07/20/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.Schaumburg@motorola.com
APT099@motorola.com

Office Action Summary	Application No.	Applicant(s)	
	10/739,354	FORS ET AL.	
	Examiner	Art Unit	
	Nicole M. Young	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 April 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Notice to Applicant

This communication is in response to the action filed on April 25, 2007. Claims 1-20 remain pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-9 and **11-19** are rejected under 35 U.S.C. 102(b) as being anticipated by **Zuk (US 5,745,571).**

Claim 1:

Column 5 lines 1-26 teaches a smart card establishing contact with a point of sale and generating a random value r. This random value is used to create an "application, master or authentication key." The key is later "used as a basis for generation of session keys for subsequent communication." The Examiner interprets the "application, master or authentication key" as the dynamic seed and the "session key" as the application key.

Claim 2:

Column 5 lines 27-29 teach that the routines used to create the random key and session keys are erased "after the authentication key and other data has been stored."

Claim 3:

Column 5 line 25 states "session keys." The Examiner interprets this as multiple keys created for different applications.

Claim 4:

Column 5, lines 1-26 teach, "providing an application seed and generating key information specific to the application."

Claim 5:

The Examiner interprets that the session key of column 5 line 25 provides a new key every time the application needs to authenticate.

Claim 6:

The Examiner interprets that the session key of column 5 line 25 corresponds to a time duration that the communication of the client and server is valid.

Claim 7:

Column 4 and 5 describe the process of generating the dynamic seed and application keys. The Examiner interprets that this process is repeated for multiple dynamic seeds and application keys.

Claim 8:

Zuk discloses multiple smart cards authenticating to the network. This teaches the Extensible Authentication protocol wherein multiple end users authenticate to a network.

Claim 9:

Column 2 lines 41-43 teach "a communications system comprising smart card means and a central processing station." The smart card is interpreted to be the client and the central processing station the network server.

Claim 11:

Column 5 lines 1-26 teaches a smart card establishing contact with a point of sale and generating a random value r. This random value is used to create an "application, master or authentication key." The key is later "used as a basis for generation of session keys for subsequent communication." The Examiner interprets the "application, master or authentication key" as the dynamic seed and the "session key" as the application key.

The Examiner interprets that this is implemented with a network access function as software. The key generation center (KGC) of these lines would be interpreted as the key manager.

Claim 12:

Column 5 lines 27-29 teach that the routines used to create the random key and session keys are erased "after the authentication key and other data has been stored."

Claim 13:

Column 5 line 25 states "session keys." The Examiner interprets this as multiple keys created for different applications.

Claim 14:

Column 5, lines 1-26 teach, "providing an application seed and generating key information specific to the application."

Claim 15:

The Examiner interprets that the session key of column 5 line 25 provides a new key every time the application needs to authenticate.

Claim 16:

The Examiner interprets that the session key of column 5 line 25 corresponds to a time duration that the communication of the client and server is valid.

Claim 17:

Column 4 and 5 describe the process of generating the dynamic seed and application keys. The Examiner interprets that this process is repeated for multiple dynamic seeds and application keys.

Claim 18:

Zuk discloses multiple smart cards, which include identity information, authenticating to the network. This teaches the Extensible Authentication protocol wherein multiple end users authenticate to a network, and it teaches Subscriber Identity Module extensions wherein the smart cards include authentication programming and identity information.

Claim 19:

Column 2 lines 41-43 teach "a communications system comprising smart card means and a central processing station." The smart card is interpreted to be the client and the central processing station the network server.

Response to Arguments

Applicant's arguments filed April 25, 2007 have been fully considered but they are not persuasive. Applicant's arguments concerning Zuk, will be addressed hereinbelow in the order in which they appear in the response filed April 25, 2007.

The Applicant states that Zuk does not discloses "obtaining, responsive to the authentication, a dynamic seed and generating an application key corresponding to the dynamic seed". The Examiner respectfully disagrees. Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

This is further described in column 5 lines 1-26, where the key generating center (KGC) decrypts the key sent to it by the card. The Examiner interprets this to be authenticating the card to the KGC, which is described in column 3 lines 20-30 to be a "central host station." The KGC then "produces an application, master or authentication K_i as a random value for the card and this is transmitted" to the card. The examiner interprets this to be obtaining a "dynamic seed" in response to authentication with a network. Column 5 lines 23-26 further states, "the application key is used in the applications which are loaded on the smart card 6, and can be used as a basis for generation of session keys for subsequent communications".

The Applicant also states the Applicant's keys are generated independently at the client and server and not exchanged, as in Zuk. The Examiner respectfully disagrees. The broadest interpretation of the claims as stated currently does not support that limitation. The Examiner interprets Pabla to anticipate all claims as stated in the above rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by **Pabla et al. (US 7,127,613)**.

Claim 1:

Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

Claim 2:

Column 6 lines 40-42 teach storing the session key for further use.

Claim 3:

Column 13 lines 1-14 teach creating groups and groups within groups with unique session keys. This is interpreted to be equivalent to a plurality of application keys where each application has a different key.

Claim 4:

Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

Claim 5:

Column 10 lines 22-28 teach using a key once per session and a new session key if the peers need to communicate again.

Claim 6:

It is interpreted by the Examiner that the session key corresponds to a time duration that the communication of the client and server is valid. This is further discussed in column 3 lines 29-41 where it states, "the two peers may use the session key for as long as the current session lasts."

Claim 7:

Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

Column 3 lines 29-41 disclose getting a new and different key when the pair needs to authenticate again.

Claim 8:

Pabla et al. discloses multiple peers authenticating to the network. This teaches the Extensible Authentication protocol wherein multiple end users authenticate to a network.

Claim 9:

Column 2 line 57 teaches a client-server environment.

Claim 10:

Column 13 lines 32-34 teach wired and wireless networks.

Claim 11:

Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second

peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

The Examiner interprets that this method is implemented as software with a network access function and key manager.

Claim 12:

Column 6 lines 40-42 teach storing the session key for further use.

Claim 13:

Column 13 lines 1-14 teach creating groups and groups within groups with unique session keys. This is interpreted to be equivalent to a plurality of application keys where each application has a different key.

Claim 14:

Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

Claim 15:

Column 10 lines 22-28 teach using a key once per session and a new session key if the peers need to communicate again.

Claim 16:

It is interpreted by the Examiner that the session key corresponds to a time duration that the communication of the client and server is valid. This is further discussed in column 3 lines 29-41 where it states, "the two peers may use the session key for as long as the current session lasts."

Claim 17:

Column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

Column 3 lines 29-41 disclose getting a new and different key when the pair needs to authenticate again.

Claim 18:

Pabla et al. discloses multiple peers authenticating to the network. This teaches the Extensible Authentication protocol wherein multiple end users authenticate to a network.

Column 7 lines 25-41 teach using the Transport Layer Security and the hardware listed in 42-53 is equivalent to a smart card.

Claim 19:

Column 2 line 57 teaches a client-server environment.

Claim 20:

Column 13 lines 32-34 teach wired and wireless networks.

Response to Arguments

Applicant's arguments filed April 25, 2007 have been fully considered but they are not persuasive. Applicant's arguments concerning Pabla, will be addressed hereinbelow in the order in which they appear in the response filed April 25, 2007.

The Applicant states that "Pabla's public key is generated only when a secured session is required, and not after authentication." The Examiner respectfully disagrees. The session is "secured" and therefore would be authenticated. Pabla column 7 lines 36-41, state that the peers authenticate to each other to "negotiate an encryption algorithm and cryptographic keys before data is exchanged." Therefore the keys are generated after the peers are authenticated. The Applicant also states the Applicant's keys are generated independently at the client and server and not exchanged, as in Pabla. The Examiner respectfully disagrees. The broadest interpretation of the claims as stated currently does not support that limitation. The Examiner interprets Pabla to anticipate all claims as stated in the above rejection.

As in the previously rejected claim 1, column 2 lines 50-67 and column 3 lines 1-11 teach two peers communicating over a network. One peer sends the other a generated public key. This is disclosed to include RSA generated public keys (column 2 lines 23-26), which is interpreted by the Examiner to be dynamic. This public key (or dynamic seed) is then used by the second peer to create a session key. This is

interpreted by the Examiner to be generating an application key. The session key is then sent to the first peer.

The Applicant states that Pabla does not disclose a "plurality of application keys" where each key corresponds to "a different application". The Examiner respectfully disagrees. The Examiner maintains the rejection of claims 3 and 13 that column 13 lines 1-14 teach creating groups and groups within groups with unique session keys. This is interpreted to be a plurality of application keys where each application has a different key. The Examiner further cites column 25 lines 55-67 and column 26 lines 1-3 teach applications with different levels of security, which is interpreted by the Examiner to be applications with different application keys based on security level.

The Applicant states that Pabla does not discloses authentication every time authentication with the network occurs. The Examiner respectfully disagrees. The Examiner interprets secured sessions to be instances of authentication as above. Pabla column 7 lines 36-41, state that the peers authenticate to each other to "negotiate an encryption algorithm and cryptographic keys before data is exchanged."

Drawings

The drawings have been amended and the objections are withdrawn.

Specification

The specification has been amended and the objections are withdrawn.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 11 and **13-20** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 11 is directed to a system entity. The specification (on page 13 paragraph 2) defines a system entity as a client or server that provides authentication services. On page 12 it states "specifically an application client." Therefore the system entity is interpreted as an application client composed entirely of software with no structural components. This is non-statutory subject matter under 35 U.S.C. 101. **Claims 13-20** are dependent claims on **claim 11** that do not further explain any structural components, therefore they are interpreted as software as well and are non-statutory.

The Examiner maintains the current 35 USC § 101 rejection. The Application states the that the system entity has "structural units such as the key manager...persistent storage unit". Each of the listed units are composed of software, except for the storage unit. Generally, functional descriptive material, such as a computer program, is statutory when it is stored on a tangible computer readable medium. See MPEP § 2106 IV.B.I(a). The claim language must include tangible structural units. The Examiner suggests, "a computer readable medium with computer instructions stored on it that causes a processor to..."

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicole M. Young whose telephone number is 571-270-1382. The examiner can normally be reached on Monday through Friday, alt Fri off, 8:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NMY
7/12/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100